FORTINET

COUNTERING THE EVOLVING CYBERSECURITY CHALLENGE WITH FORTINET SECURITY FABRIC

WHITE PAPER

COUNTERING THE EVOLVING CYBERSECURITY CHALLENGE WITH FORTINET SECURITY FABRIC

The emerging digital economy drives business value by leveraging technology to connect users, devices, data, goods, and services. To compete successfully, organizations are required to adopt new models of connectivity and data sharing, including public and private clouds and enabling the Internet of Things (IoT). These new approaches enable organizations to be more agile, more responsive to customer needs and market demands, enhance competitive differentiation, and expand their global market footprint.

The adoption of a digital business model is requiring networks to evolve rapidly, requiring applications, data, and services to flow faster across an increasingly diverse landscape of users, domains, and devices As a result, today's networks and their related security are also increasingly borderless. IoT and cloud applications, services, and infrastructure now require organizations to worry about an attack surface that may not even be visible to IT.

The irony of this network evolution is that as we make applications, data, and services flow faster across an increasingly diverse landscape of users, devices, and domains, we are also compounding the complexity of securing this new environment against an ever-changing threat landscape.

Today, we face a huge volume of cyber threats along with highly sophisticated targeted attacks, made possible by the commercialization of a whole ecosystem of cybercrime services and supply chain resources and services.

And in addition to securing themselves against these threats, organizations must also document and demonstrate the measures they are taking to meet evolving regulatory and compliance requirements. Because risk is accelerating, governing bodies all over the world are mandating risk management processes. Implementing these is an arduous task—compliance requires auditing, monitoring, and adherence—and the complexity of these processes is compounded as the network becomes more and more distributed.

To date, the common approach has been to keep adding new security devices to an already overburdened security closet. But as the continued increase of network compromises indicates, this approach isn't solving the problem. The fact is that while the new devices you are buying and deploying are helping to decrease the time it takes to discover some new threats, data shows that threats are compromising organizations even faster. You just can't keep up using this approach.

Siloed security solutions, with separate management interfaces and no meaningful way to gather or share threat information with other devices on your network, are only marginally useful.

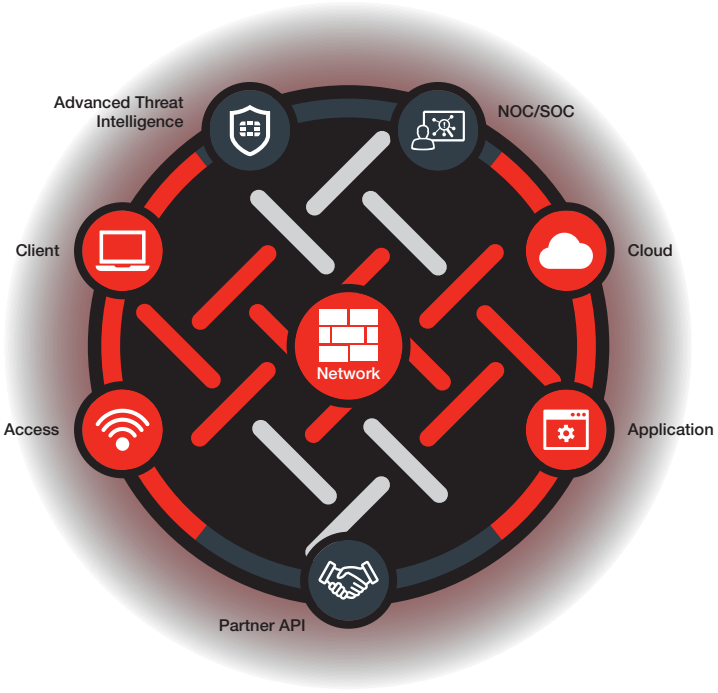
A NEW APPROACH

But what if the data and security elements across all of an organization's various environments could be well-integrated, cohesive, and coherent, like a seamlessly woven fabric? Such an approach would allow companies to see, control, integrate, and manage the security of their data across their entire organization, even into the cloud, enabling a secure digital business model.

Such an approach would also allow security to dynamically expand and adapt as more and more workloads and data are added, and at the same time, seamlessly follow and protect data, users, and applications as they move back and forth between IoT and smart devices, borderless networks, and cloud-based environments.

THE FORTINET SECURITY FABRIC

The Fortinet Security Fabric provides a new, intelligent architectural approach to security that, for the first time, enables enterprises to weave together all of their discrete security solutions into an integrated whole. This fabric-based approach is built around three key attributes:



1.Broad

The Security Fabric is designed to cover the entire attack surface. Security solutions deployed across the network cannot stand alone as isolated devices. To secure today's networks, administrators must have visibility across the entire environment, including endpoints, access points, network elements, the data center, the cloud, and even the applications and the data itself.

Comprehensive visibility across the distributed enterprise ties together data, applications, devices, and workflows to provide a level of awareness and responsiveness, managed through a single pane of glass, which has never before been available from any security provider. Awareness of each network element, including solutions from other vendors, as well as how data flows between them, enables administrators to find and respond to even the most sophisticated threats.

Combined with dynamic network segmentation that logically separates data and resources, the Security Fabric can see deep into the network to discover threats as they move from one network zone to the next. Such broad deployment and deep visibility aids in compliance, helps monitor internal traffic and devices, prevents unauthorized access to restricted data and resources, and controls the spread of intruders and malware.

2.Powerful

With the performance requirements demanded by today's networks, security not only needs to be pervasive, but extremely powerful as well. Today's digital businesses cannot afford to trade protection for performance in any segment of the network. They also cannot afford to harden one attack vector while leaving another wide open, or leave even one user or application unprotected.

Furthermore, the same strong security must be deployed at the endpoint for devices, embedded at the access layer for wired and wireless network access, scale from the smallest branch deployments to the largest, most complex and data-intensive campus and data center environments, and be available virtually to protect the private, hybrid, and public cloud.

Fortinet security solutions are based on the fastest, purpose-built security processing units (SPUs) in the industry to reduce the burden on infrastructure, as well as highly optimized software versions, allowing organizations to establish comprehensive security without affecting performance. And as part of the Security Fabric, physical and virtual security technologies can be woven together to scale policy and enforcement across your entire distributed network, allowing you to more effectively secure your evolving network environment while solving new threat challenges.

3.Automated

The Fortinet Security Fabric enables a fast and coordinated response to threats, allowing all elements to rapidly exchange threat intelligence and coordinate actions. But because an attack can compromise a network in minutes, visibility isn't enough. The network also needs to be able to respond at the speed of the attack. So not only do security solutions need to be able to correlate threat intelligence to determine the level of risk, they also need to automatically synchronize a coordinated response. The Security Fabric can dynamically isolate affected devices, partition network segments, update rules, push out new policies, and remove malware.

Security solutions also need to dynamically adapt to changing network configurations and establish and enforce new policies as the environment being protected adapts to shifting business needs. Security measures and countermeasures need to be provisioned automatically as new devices, workloads, and services are deployed anywhere, from remote devices to the cloud.

AN INTEGRATED AND COLLABORATIVE APPROACH

The Fortinet Security Fabric connects critical security and networking technologies—from firewalls to content and application security to secure access points—for seamless security across the distributed network, whether local or remote, physical or virtual, wired or wireless, and in your domain or in the cloud.

Enterprise Firewalls—The Fortinet Security Fabric's core foundation is built on Fortinet's Enterprise Firewalls—for branch, campus, data center, and internal segmentation deployment—all interconnected by a single, unified operating system for simplified and coordinated deployment and control. This architecture actually delivers the benefits of standardization claimed by many "platform" vendors.

Enterprise firewall capabilities can be scaled from the branch, to the campus, and into the data center, providing the industry's highest-performing, most secure defense against known threats. Additionally, the Enterprise Firewall solution allows segmentation of network elements, enforcing traffic, device, and data separation for stronger control. And, as new threats become known, all firewalls in the environment can be dynamically updated to protect against them.

Cloud Security—As enterprise networks expand, the Fortinet Security Fabric can scale deep into the cloud. Virtual firewalls can be deployed in your private cloud, as well as in your public cloud IaaS environments, for north-south and east-west microsegmentation. Coupling Fortinet's Cloud Security with your existing enterprise firewall deployment seamlessly extends the same powerful security at scale, as well as the same intelligence and dynamic risk mitigation to applications located either in the cloud or on-premise.

Advanced Threat Protection—Of course, detecting known threats is only half the battle. Fortinet's Advanced Threat Protection solutions can detect and mitigate previously unknown threats, sharing global and local intelligence across security elements in the

Security Fabric. They are designed to work together to automatically and continuously hand off data from one to the next to prevent, detect, and mitigate attacks across the entire environment and all attack vectors.

Application Security—The Fortinet Security Fabric ensures the security and availability of your web-based applications that have long been favorite targets of hackers because they have access to valuable information and historically have been relatively easy to exploit. A successful attack can result in a variety of devastating consequences including financial loss, damage to brand reputation, and loss of customer trust. Fortinet's application security solution delivers a complete, single-vendor solution with the proven performance and security effectiveness required to meet the increasing demands of today's applications.

Secure Access—The Fortinet Security Fabric goes well beyond just integrating security solutions. Our Secure Access solution extends the coordinated security policies to the very edge of the wired and wireless network where most vulnerabilities are targeted.

Security Operations—Adaptive visibility and control across the Fortinet Security Fabric is a requirement for the security operations team tasked with monitoring and responding to incidents throughout the organization. A range of tools is available to manage, monitor, and report on multiple fabric components from one place, whether they are multiple instances of the same Fortinet product, multiple Fortinet products, or multiple products across multiple vendors.

Fabric-Ready Partners—In addition to the native integrations built between Fortinet's portfolio of security solutions, the Fortinet Security Fabric also supports open application programming interfaces (APIs), open authentication technology, and standardized telemetry data. These allow organizations to integrate existing security and networking investments into the Fortinet Security Fabric. Fortinet has developed a growing ecosystem of Fabric-Ready Partners whose solutions have been certified to operate within the Fortinet Security Fabric framework.

SUMMARY

The evolving enterprise and its transition to a digital business model is one of the most challenging aspects of security today. As significant trends in computing and networking continue to drive changes across critical business infrastructures, architectures, and practices, organizations are looking for innovative network security solutions to help them embrace that evolution.

The Fortinet Security Fabric is an intelligent framework designed around scalable, interconnected security combined with high awareness, actionable threat intelligence, and open API standards for maximum flexibility and integration to protect even the most demanding enterprise environments. Fortinet's security technologies have earned the most independent certifications for security effectiveness and performance in the industry. When woven together, the Fortinet Security Fabric closes gaps left by legacy point products and platforms by providing the broad, powerful, and automated protections today's organizations require across their physical and virtual environments, and from endpoint to the cloud.

For more information on the Fortinet Security Fabric, please visit our website.

GLOBAL HEADQUARTERS
Fortinet Inc.
899 Kifer Road
Sunnyvale, CA 94086
United States
Tel: +1.408.235.7700
www.fortinet.com/sales

EMEA SALES OFFICE
905 rue Albert Einstein
06560 Valbonne
France
Tel: +33.4.8987.0500

APAC SALES OFFICE
300 Beach Road 20-01
The Concourse
Singapore 199555
Tel: +65.6513.3730

LATIN AMERICA HEADQUARTERS
Sawgrass Lakes Center
13450 W. Sunrise Blvd., Suite 430
Sunrise, FL 33323
Tel: +1.954.368.9990

Dec 30, 2016